Proposed New Mechanism to Detect and Defend the Malicious Attackers in AODV

Vijay Kumar[1], Ashwani Kush
[1]Department of Computer Science & Applications,
IEC University, Baddi (Solan). H.P. – INDIA
vk.gnkc@gmail.com
[2]Department of Computer Science & Applications,
University College, Kurukshetra University, Kurukshetra-INDIA
akush20@gmail.com

Abstract

In MANETs to protect a network layer from malicious attacks is an important and challenging security issue. In this paper, A new mechanism has been proposed to detect and defend the network against such attack which may be launched cooperatively by a set of malicious nodes. The proposed algorithm has been incorporated on AODV routing protocol. The proposed algorithm does not use any cryptographic primitives on the routing messages. But, it is protecting the network by detecting and deactivating the malicious activities of node. Simulations have been carried out using NS2. Simulation results show that the proposed algorithm encouraging results.

Keywords: *Mobile ad hoc networks, malicious attack, routing misbehavior.*

1. Introduction

Due to recent performance advancements in computer and wireless communicative technologies, mobile wireless computing is becoming increasingly widespread. One type of wireless network that is quickly evolving is the Mobile Ad Hoc Network (MANET). Unlike other mobile network paradigms, such as cell phone networks with fixed radio towers and centrally accessible routers and servers, MANETs have dynamic, rapidly-changing, random, multi-hop topologies composed of bandwidth, constrained wireless links and no centrally accessed routers or servers.

While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are either absent or less severe in wired networks. MANETs are vulnerable to various types of attacks including passive eavesdropping, active interfering, impersonation, and denial-of-service. Intrusion prevention measures such as strong authentication and redundant transmission should be complemented by detection techniques to monitor security status of these networks and identify malicious behavior of any participating node(s). The rest of the paper is organized as follows. Section II describes Statement of the problem. Section III describes the Malicious Node Detection Process Using Proposed Modi_AODV. Section IV presents the simulations and the performance analysis of the scheme. Section V concludes the paper.

2. Statement of the Problem

Recently, the use of deceptive mechanisms for security and stability has become very common in wired and infrastructure based wireless networks. They have traffic concentration and control points such as switches, routers or gate ways where wired/ wireless resources are deliberately deployed to lure and capture the attackers. MANET does not have such concentration or control points, therefore no proper architecture has been proposed till now for use of deceptive techniques in MANETs. However, the specific features of deception techniques like reliability, control over deployed resources and their luring capabilities can be used overcome the limitations of earlier security schemes used in general ad-hoc environment.

3. Malicious Node Detection Process Using Proposed Modi_Aodv

The basic idea of the Modi_AODV protocol is to identify and detect the malicious node using the proposed algorithm and select all possible alternative routes to a target node that does not pass through the malicious node from the source to destination node. In modi_AODV protocol, the numbers of various paths from the source node to the destination node are determined based on the number of edges emitting from the source node. Afterwards these messages will be delivered through the several other paths detected by the algorithm. The selection process is conducted in sequential path. In Modi_AODV it is assumed that the malicious node will

not succeed to disrupt communication between the source and the destination nodes.

Proposed Algorithm to Detect and Reactivate Malicious Nodes

The following assumptions are taken to design the proposed algorithm.

1. A node interacts with its 1-hop neighbours directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
2. Every node has a unique ID in the network, which is assigned to a new node collaboratively by existing nodes.
3. The network is considered to be layered.
4. Source and Destination node will not be malicious node.

Steps of Modi_AODV Algorithm

Algorithm section 1: Working of RREQ packet

Step 1: Set htype "0" or "1"

Htype = "0" means non malicious node

Htype = "1" means malicious node

Step 2: Broadcast RREQ packet (p) by source node

Step 3: if node htype = "0" then broadcast RREQ to this node

If htype = "1" then deactivate this node and don't broadcast RREQ

Step4: repeat steps 2 and 3 until it reaches the destination

Algorithm Section2: Working of RREP packet

Step 1: Destination node rebroadcast the RREP packet like the RREQ

Step 2: All the possible routes will be searched by RREP

Step 3: If any node is out of signal range or dead from the network after getting RREQ then available route will be selected by the RREP broadcasting. No need to rebroadcast RREQ and then re- reply for select the routing path

Step 4: repeat steps 2 and 3 until it reaches to source node

Step 5: Source node will select all the possible paths for data transmissions to destination node.

Algorithm Section 3: Data Packet Transmission

Step 1: Select all the possible paths from source to destination to send the data packets.

Step 2: Distribute all the data packets on every event and send them equally through the selected paths at this event.

Step 3: source node receives overhearing from destination node after receiving data packets from all selected routes.

Step 4: If source node does not receives overhearing message for any selected route than this route will be discarded from the routing table and assume the presence of malicious node in this route.
Step 5: After detecting the malicious nodes it is discarded from routing table and it will not be included in the selected route for further event.

4. Comparative Simulation Results Between AODV and Modi_AODV

The working of routing largely depends upon successful transmission of packets to the destination. This requires proper selection of Routing path and algorithm. AODV and Modi_AODV have been used for routing solutions. All the simulations have been performed using Network Simulator NS-2.32 on the platform Fedora 13. The traffic sources are CBR (Continuous Bit Rate). The source-destination pairs are spread randomly over the network. During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes time to rest and than second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. Different network scenario for varying number of nodes and distinguished node transmission range are generated.

Table 1: Evaluation Parameters

Simulation Parameters	Parameter Value
Simulator	NS-2.32
Routing Protocol	AODV and Proposed Modified AODV
Communication Type	CBR
Number of Nodes	10, 20, 50
Maximum mobility speed of nodes	0,4,6,8,10 m/sec
Simulation Area	1000m x 1000 m
Simulation Time	500 sec
Packet Size	512 bytes
Number of malicious nodes	1, 2, 4

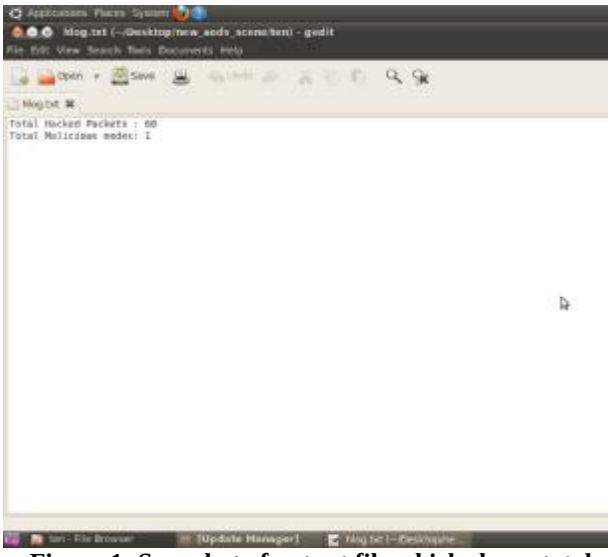

Figure 1: Snapshot of output file which shows total attackers and dropped packets with 10 Nodes scenario.

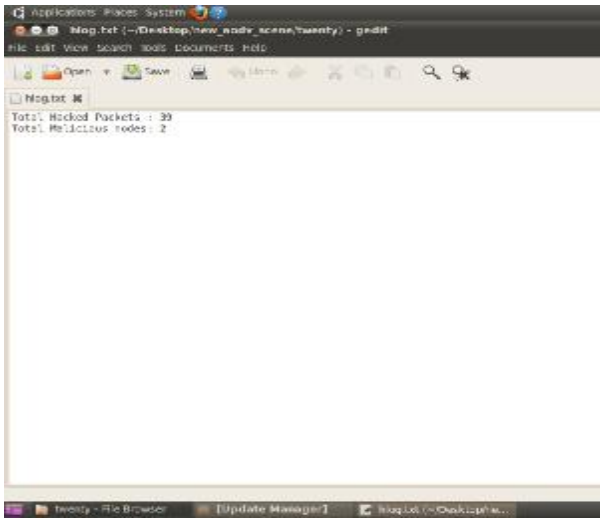

Figure 2: Snapshot of output file which shows total attackers and dropped packets with 20 Nodes

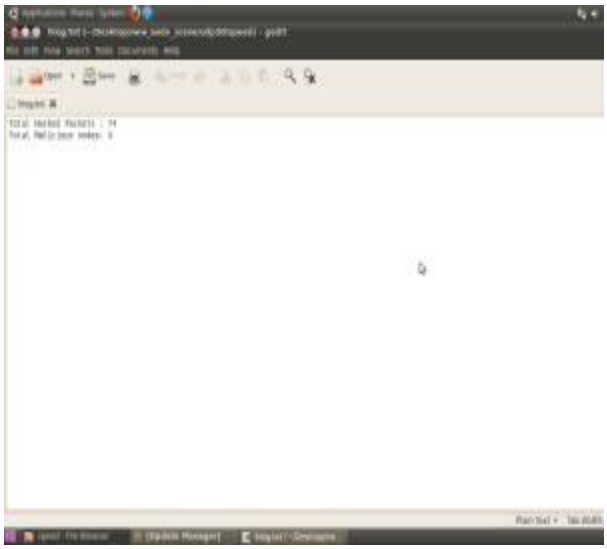

Figure 3: Snapshot of output file which shows total attackers and dropped packets with 50 Nodes

Figure 4: Snapshot of NAM file which shows movement of nodes and dropping packets with 50 Nodes

5. Statistical Evaluation of Simulation Results

Table 2: % Overhead

	10 Nodes		***20 Nodes***		***50 Nodes***	
Parameters	***AODV without Malicious Attack and AODV with malicious attack***	***AODV without Malicious Attack and Modi_AODV with malicious attack***	***AODV without Malicious Attack and AODV with malicious attack***	***AODV without Malicious Attack and Modi_AODV with malicious attack***	***AODV without Malicious Attack and AODV with malicious attack***	***AODV without Malicious Attack and Modi_AODV with malicious attack***
Packet Delivery Ratio	20.536	0.482	19.704	0.706	20.74721302	0.946068093
Throughput	22.55081	1.4763	19.33919518	0.405205372	20.99772417	1.71476344
End to End Delay Ratio	0.000168	124.147	22.88067898	99.05142287	47.44427457	17.305314

In Table 2, % Overhead shows. % Overhead in packet delivery ratio in all three scenarios, Modi_AODV with malicious nodes has very less i.e. 0.482 to 0.946068093 in comparison of AODV with and without malicious nodes i.e.19.704 to 20.74721302.

% Overhead in throughput in all three scenarios, Modi_AODV with malicious nodes has very less i.e. 0.405205372 to 1.71476344 in comparison of AODV with and without malicious nodes i.e.19.33919518 to 22.55081.

% Overhead in end to end delay ratio is less in 50 nodes scenario in Modi_AODV with malicious nodes i.e. 17.305314 in comparison of AODV with and without malicious nodes i.e.47.44427457. But in remaining two scenarios its very high in Modi_AODV with malicious nodes.

In Table 3, % Overhead shows of data packets sent and received. That table shows AODV without malicious attack gives very good results i.e. 0 to 0.483351235 But the results with malicious attacks in AODV are not good i.e. 19.82759 to 24. Again in Modi_AODV with malicious attacks results are good i.e. 0.477327 to 1.32231405.

In Table 4 shows Co-efficient of correlation. In packet delivery ratio correlation between AODV without and with malicious attacks in all three scenarios lies between low negative to high negative. On other hand correlation between AODV without malicious nodes and Modi_AODV with malicious nodes in all three scenarios lies between low positive to moderate positive.

Table 3: % Overhead

	10 Nodes			20 Nodes			50 Nodes		
Parameter	*AODV without Malicious Attack Data Packet Sent and Received*	*AODV with malicious attack Data Packet Sent and Received*	*Modi_AODV with malicious attack Data Packet Sent and Received*	*AODV without Malicious Attack Data Packet Sent and Received*	*AODV with malicious attack Data Packet Sent and Received*	*Modi_AODV with malicious attack Data Packet Sent and Received*	*AODV without Malicious Attack Data Packet Sent and Received*	*AODV with malicious attack Data Packet Sent and Received*	*Modi_AODV with malicious attack Data Packet Sent and Received*
Data Packets Sent and Received	0	24	0.477327	0	19.82759	0.719424	0.483351235	20.8652793	1.32231405

Table 4: Co-efficient of Correlation

	10 Nodes		20 Nodes		50 Nodes	
Parameters	*AODV without Malicious Attack and AODV with malicious attack*	*AODV without Malicious Attack and Modi_AODV with malicious attack*	*AODV without Malicious Attack and AODV with malicious attack*	*AODV without Malicious Attack and Modi_AODV with malicious attack*	*AODV without Malicious Attack and AODV with malicious attack*	*AODV without Malicious Attack and Modi_AODV with malicious attack*
Packet Delivery Ratio	-0.999398703	0.516905611	-0.112685559	0.508510726	-0.065082862	0.289847356
Throughput	-0.082760129	0.465276591	0.919687004	0.998570886	0.967430467	0.982844094
End to End Delay Ratio	0.492062764	0.759453643	0.873056475	0.703326942	-0.350595376	0.877024364

Co-efficient of correlation in throughput between AODV without and with malicious attacks in all three scenarios lies between low negative to high positive. On other hand correlation between AODV without malicious nodes and Modi_AODV with malicious attack in all three scenarios between low positive to high positive.

Co-efficient of correlation in end to end delay ratio between AODV without and with malicious attacks in all three scenarios lies between low negative to high positive. On other hand correlation between AODV without malicious nodes and Modi_AODV with malicious attack in all three scenarios between moderate positive to high positive.

Throughput (0.601452 and 0.815564) and end to end delay ratio (0.338175 and 0.779935).

6. Summary

- Mean of % overhead is very less in Modi_AODV in comparison of AODV in packet delivery ratio and throughput i.e. 0.711356, 1.198756 and 20.32907, 20.96258, but with end to end delay ratio %overhead is very high in Modi_AODV in comparison of AODV i.e. 80.016791 and 23.44171. It proves that end to end delay ratio is high in Modi_AODV.
- Mean of coefficient of correlation is better in Modi_AODV in comparison of AODV i.e. packet delivery ratio (-0.39239 and 0.438421),

References:

[1]. Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE communications surveys & tutorials, Vol. 10, no. 4, pp. 78- 93, 2008.

[2]. Arshad, J.; Azad, M.A.; , "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks", Sensor and Ad Hoc Communications and Networks, SECON '06. 2006 3rd Annual IEEE Communications Society on, vol.3, no., pp.971-975, 28-28 Sept. 2006.

[3]. Ye Tung; Alkhatib, M.; Rahman, Q.S.,"Security Issues in Ad-Hoc on Demand Distance Vector Routing (AODV) in Mobile Ad-Hoc Networks", Proceedings of the IEEE , vol., no., pp.339-340, 2005.

[4]. Payal N. Raj, Prashant B. Swadas, "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Bodv Based Manet", In: International Journal of Computer Science Issues, Vol.2, pp 54-59, 2009.

[5]. A.Kush, R.Chauhan,C.Hwang and P.Gupta, "Stable and Energy Efficient Routing for Mobile Adhoc Networks", Proceedings of the Fifth International Conference on Information Technology: New Generations, ISBN:978-0-76953099-4 available at ACM Digital Portal, pp. 1028-1033, 2008.

[6]. C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[7]. Harris Simaremare and Riri Fitri Sari, "Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011.

[8]. Vijay Kumar and Ashwani Kush, " Detection and Recovery of Malicious Node in Mobile Ad Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 1, January 2012 ISSN: 2277 128X .

First Author: Vijay Kumar is employed as Assistant Professor in Department of Computer Science & Applications, I.E.C. University, Baddi (Solan) H.P. India. He has 9 years teaching experience. He has done MCA, M.Phil and Ph.D.(Pursuing) in Computer Science. He has 18 research papers to his credit in various International/National Journals and Conferences. His research interests are in Mobile Ad hoc Networks.

Second Author : Dr. Ashwani Kush is employed as Head and Associate Professor in Department of Computer Science & Applications, University College, Kurukshetra University, Kurukshetra. He has done Ph.D. in Computer Science in association with Indian Institute of Technology, Kanpur, India and Kurukshetra University, Kurukshetra, India. He is professional Member of ACM, IEEE, SCRA, CSI INDIA and IACSIT Singapore, IAENG Hon Kong. He has more than 60 research papers to his credit in various International/National Journals and Conferences. He has authored 15 books in computer science for undergraduate and school students. His research interests are in Mobile Ad hoc Networks, E-Governance and Security. Dr. Kush has chaired many sessions in International Conferences in USA and Singapore. He is member of Syllabus Committee, Time table and Quiz Contests of Kurukshetra University, Kurukshetra, India. He is also on the panel of eminent resource persons in Computer Science for EDUSAT project, Department of Higher Education, Government of Haryana. His lectures are also broadcasted through satellite in Haryana, India.